附件 2

# 团体标准《面向 5G 通信网络的异常数据生成与信流检测技术规范》编制说明

## 一、工作简况

（一）任务来源：2024 年 12 月，由重庆邮电大学牵头开始本标准的工作，于 2025 年 3 月广东省质量检验协会发布立项。。广东省质量检验协会提出和归口，重庆邮电大学等单位共同起草，完成期限为 18 个月。

（二）协作单位：本标准由广东省质量检验协会提出并归口，参与起草单位有重庆邮电大学、深圳北理莫斯科大学、香港大学、中国检验检疫科学研究院粤港澳大湾区研究院、广州波奇亚标准及检测技术有限公司、澳门科技大学、OrionAI Limited、中山市信裕科技有限公司、中山市政达企业管理服务有限公司。

（三）具体分工：广东省质量检验协会作为本标准的牵头指导单位，主要负责本标准的总体工作方向、实施方案与基本框架的确认，重庆邮电大学作为本标准的主导起草单位，负责标准项目的策划组织和实施推进，按照标准制定程序实施标准研制，论证标准关键内容，开展标准宣传推广普及等。深圳北理莫斯科大学、香港大

学、中国检验检疫科学研究院粤港澳大湾区研究院、广州波奇亚标准及检测技术有限公司、澳门科技大学、OrionAI Limited、中山市信裕科技有限公司、中山市政达企业管理服务有限公司作为本标准的主要参与单位，负责组织行业专家开展标准的调研、起草、编制与论证工作，各协作单位利用各方发挥自身专业优势、人员优势，形成专业+标准的工作模式，全面确保标准的科学性、准确性、完整性与应用性。

## 二、立项的必要性

通信网络的异常数据生成与信流检测的核心问题在于其高效性、准确性、实时性和隐私保护等特征。通过自动化和多模态数据融合技术，为网络运营商提供可信、连续的异常数据检测与信流分析手段，提升网络的安全性、稳定性和性能。该技术弥补了传统基于人工检测和经验分析的局限，满足了网络环境下动态流量监测与应急处理的需求，促进了网络安全防护、故障诊断与恢复的及时性，并平衡了大规模数据分析与用户隐私保护的要求。此技术的实施旨在统一关键指标和技术规范，鼓励系统开发者和服务提供方共同构建安全、高效且注重隐私保护的异常数据生成与信流检测体系，为通信网络的可持续发展提供有力保障。

## 三、标准框架和内容的确定

（一）标准框架

本标准结合我国现有政策、法规与标准，遵循和按照国家标

准 GB/T 1.1-2020《标准化工作导则 第 1 部分：标准化文件的结构和起草规则》的要求统一和规范标准的结构、表述规则、编排格式和制定程序，坚持市场导向原则，鼓励企业参与制定标准，提高标准的适用性；坚持国际化原则，积极采用国际标准，保持与国际并行的步伐；坚持科学严谨的原则，系统深入研究心理状态监测方法的科学性。

（二）主要内容

本文件主要包括以下方面内容:

1. 范围

本文件规定了通信网络的异常数据生成与信流检测的要求，数据的获取，生成原理，实验方法，信流分析机制，传输，重组等内容。

本文件适用于面向 5G 通信网各类通信协议的异常数据生成与信流检测技术。包括面向 5G 用户面流量生成任务的异常数据模拟生成系统，也适用于基于信令流量的信令网异常检测技术研究。

2. 规范性引用文件。

规范性引用文件中列示了本标准引用的相关标准。本标准中引用了 12 个国家标准，均为推荐性标准。

3. 术语和定义。

为便于对本标准的理解和适用，本部分对标准中涉及的主要术语进行了定义。同时指明 GB/T 25069-2022、GB/T 22239-2020、GB/T 37988-2019、ISO/IEC 27001:2013、3GPP TS 29.501 5G、IEEE 5G、Free5GC、Hyperledger Fabric、RFC 5246 TLS、ITU-T X.805、T/CCSA 20004-2018 5G、RFC 8705 OAuth 2.0 界定的术语同样适用于本文件。

4. 异常数据生成与检测方法

给出了异常数据生成方法和异常信流检测方法。通过异常数据生成，系统能够模拟各种潜在的网络攻击流量，为异常检测系统提供多样化的训练数据。通过异常信流检测，帮助检测系统区分正常流量和异常流量，识别如 DDoS 攻击、协议滥用等复杂的异常行为，及时发现潜在的异常信流。

5. 技术要求。

给出通信网络的异常数据生成与信流检测的技术要求。主要基本要求、数据质量要求、生成模型技术要求、检测模型技术要求、设备与系统要求等作出规定。

6 数据生成与特征提取。

给出通信网络的异常数据生成与信流检测的平台搭建规范，以及数据采集与预处理、特征提取与表征的规范，包括数据处理和模型设计流程，保证数据的质量和安全。

数据采集与预处理规定数据采集过程应通过5G通信网的核心网及用户面网元收集流量数据，采集的数据应包括正常流量数据和已知的攻击流量数据。数据应以PCAP格式存储，并通过专用通道传输到远程服务器进行后续处理。采集到的原始数据应经过数据清洗、特征提取和标准化等预处理步骤。特征提取包括从原始流量中提取关键特征，如数据包大小、传输速率、时序特征等。所有特征应标准化，确保生成模型能够处理具有相同尺度的输入数据。特征选择应依赖于5G通信网的流量协议和攻击类型，重点提取有助于识别异常流量的关键指标。

数据存储流程章节规定了提取的特征应能够全面表征信令流的状态，并涵盖不同类型的流量，包括正常流量与攻击流量。在特征提取后，需对数据进行标准化处理，以确保不同特征的数值范围一致，避免在后续模型中产生偏差。

## 四、与现行法律法规、强制性标准等上位标准关系

本文件符合国家现行法律、法规、规章和强制性国家标准的要求，本标准有助于国内相关法律、法规、规章和强制性国家标准的实施。

## 五、标准有何先进性或特色性

本标准在充分研究标准化有关法律法规和标准化政策方向的基础上，在异常流量检测与数据采集方面具有重大创新。一是基于

**开源平台构建**，采用 Free5GC 平台，实现 5G 核心网的灵活配置和扩展，提升了系统在多样化应用场景下的适应性。二是**全面多功能集成**，标准不仅涵盖了接入管理、会话管理、网络切片等核心网功能，还集成了异常流量数据采集与预处理，为后续的攻击识别提供了高质量的数据基础。三是**特征提取与分析多维度**，全面从数据包大小、传输速率等多个维度进行特征提取，精准区分正常流量与攻击流量，提升了流量异常检测的准确性。四是**生成对抗网络与强化学习结合**，采用生成对抗网络模型与强化学习机制，优化生成的异常流量样本质量，通过博弈式训练不断提高检测模型的辨识能力，确保系统在复杂攻击场景中的有效性。

**六、标准调研、研讨、征求意见情况**

**（一）项目启动。**2024 年 12 月重庆邮电大学受委托承担了本标准的制定工作，联合深圳北理莫斯科大学、香港大学、中国检验检疫科学研究院粤港澳大湾区研究院、广州波奇亚标准及检测技术有限公司、澳门科技大学、OrionAI Limited、中山市信裕科技有限公司、中山市政达企业管理服务有限公司，成立标准编制工作组（以下简称工作组）。工作组明确了工作组的责任和要求，讨论和确定了详细的人员分工和工作计划，包括时间计划和流程规划。工作组开始广泛调研相关的法律法规和整理思路。

**（二）广泛调研。**2024 年 12 月，工作组广泛搜集、整理和分

析相关的法律法规，国家、行业和地方标准，调研相关的技术文献，整理标准制定思路，形成标准的基本框架。

**（三）形成征求意见稿。**2024 年 12 月至 2025 年 1 月，各参编单位根据自身优势参与标准草案的不同部分编制工作，编制组召开 3 次标准讨论会，会上对标准草案的基本架构、主要内容和技术要求等内容进行反复讨论和修改。

**（四）征求意见。**2025 年 1 月，经过前期多次修改讨论，形成征求意见稿。征求意见稿在具有通信、安全等相关领域研究和应用经验的高校、企业、行业协会和标准相关部门发送。截至 2025 年 3 月，收集汇总相关的意见 20 条，经主编单位分析后，采纳意见 18 条，部分采纳意见 2 条，未采纳意见 0 条。“部分采纳”的处理结果向意见提出单位进行反馈，最终达成一致。

## 七、技术指标设置的科学性和可行性

本文件的指标科学性和可行性体现为：一是技术指标设置科学合理。本标准是在充分分析国家标准、行业标准对生物特征、数据融合等相关要求的基础上提出异常数据生成与信流检测规范，并在此基础上开展了大量的面向 5G 通信网络的异常数据生成与信流检测技术的调研，结合相关数据的出来的技术指标，不仅满足法律法规和标准要求，还结合企业实际，具有科学性。二是技术指标具有及时性和前瞻性。本标准提出从技术要求和数据使用的多个细节规范方面提出了适

应现时市场需求和未来技术发展的技术指标，有助于引导面向5G通信网络的异常数据生成与信流检测技术的规范化发展，具有可行性。

**八、与国际、国家、行业、其他省同类标准技术内容的对比情况，或者与测试的国外样品、样机的有关数据对比情况。采标情况，以及是否合规引用或采用国际国外标准**

截至目前，还没有面向5G通信网络的异常数据生成与信流检测技术规范相关的国际、国家、行业、其他省同类标准。

**九、涉及专利的有关说明**

无。

**十、专家审定会情况**

/

**十一、标准名称变更应详细说明理由并单独拟文申请**

无。

**十二、编制单位增减应予说明增减原因并单独拟文申请**

无。

**十三、其他应当说明的事项**

无。

标准编制工作组

2025年3月10日